UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/829,571	04/22/2004	Yen-Fu Chen	AUS920040043US1	6336

45993 7590 06/18/2007

IBM CORPORATION (RHF)
C/O ROBERT H. FRANTZ
P. O. BOX 23324
OKLAHOMA CITY, OK 73123

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
06/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/829,571	CHEN ET AL.	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/22/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending in this application.

2. Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Objections

3. Claims 2, 9 and 16 are objected to for lack of antecedent basis:

Claim 2 recites "the next unused pad" in line 4.

Claim 9 recites "the next unused pad" in line 5.

Claim 16 recites "the next unused pad" in line 5.

Appropriate correction and/or clarification required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7-12, 14-19 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shefi (Patent No.: US 6,445794 B1) in view of Muller (Klaus Muller, Siemens AG, "Intermediate report on UMTS security mechanisms: USECA"; April 1999, p. 1-73).

6. As to claim 1, Shefi disclose a system for authenticating a client device requesting a session of service from a service provider (abstract), comprising:

at least two matching one-time pad cryptological tables (column 4, lines 5-15, "...an identical electronic one-time pad at a first location and at a second location"), a first of which is stored in a client device ("a first electronic device" – e.g. column 4, lines 5-20), and a second of which is accessible by a service security server ("a second electronic device" – e.g. column 4, lines 5-15), each table having multiple entries (column 11, lines 13-30, "...a true number is selected from at least one table containing true random number is selected from at least one table containing true random numbers..."), each entry including a field for a indicator of previous use (column 11, lines 10-30, "..table containing true random numbers according to a pointer"), said previous use indicator for each entry being initialized in an "unused" state (Shefi

teaching this concept by selecting true random number that is identical at all locations – e.g. column 11, lines 10-30), each row containing at least one pad value ("random number" –e.g. column 11, lines 10-.30);

Shefi doesn't explicitly disclose a code exchanger for receiving a pad value from said client device by said service security server upon request for initiation of a service session; a code comparator for determining if said received pad value is marked as "used" or "unused" in said second table; a service session grantor configured to grant said service request responsive to determination that said received pad value is unused, including changing said used indicator to a "used" state upon said grant of service; and a client device reconfigurator adapted to challenge said user of said client device responsive to determining that said received pad value is marked as "used", and to replace said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge.

However, Muller discloses a code exchanger for receiving a value from said client device by said service security server upon request for initiation of a service session (page 13, Muller teaches this concept by disclosing "A sequence number as time variant parameter only provides assurance to B that the evidence was not used in a previous protocol run"); a code comparator for determining if said received value is marked as "used" or "unused" in said second table (page 13, "..assurance to B that the evidence was not used in a previous run"); a service session grantor configured to grant said service request responsive to determination that said received value is unused (page 13 and page 16, "...the SN checks that RES and XRES are the same. If they are

not, authentication has failed and access is denied."), including changing said used indicator to a "used" state upon said grant of service (page 13, Muller teaches this concept in order to assure to B that the evidence was not used in a previous run, -e.g. page 13); and a client device reconfigurator adapted to challenge said user of said client device responsive to determining that said received value is marked as "used" ("authentication challenge" –e.g. page 16, page 46), and to replace said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge (page 18, 46, "A special re-synchronization procedure may be used to recover..").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Shefi as taught by Muller in order to provide integrity protection of signaling messages and on user traffic confidentiality over the wireless network.

7. As to claims 8 and 15, these are rejected using the same rationale as for the rejection of claim 1.

8. As to claim 2, Shefi discloses wherein: said one-time pad cryptological tables further comprise a sequence index (column 11, lines 10-30, "..table containing true random numbers according to a pointer"). Shefi doesn't explicitly disclose said code comparator is further configured to determine if said received pad is the next unused pad according to said sequence indicators; said session grantor is configured to grant a

session only if said received pad is a next expected pad; and said client device reconfigurator is adapted to respond to said received pad not being a next expected pad.

However, Muller discloses disclose said code comparator is further configured to determine if said received pad is the next unused pad according to said sequence indicators (page 13, "..assurance to B that the evidence was not used in a previous run"); said session grantor is configured to grant a session only if said received pad is a next expected pad (page 13 and page 16, "...the SN checks that RES and XRES are the same. If they are not, authentication has failed and access is denied."); and said client device reconfigurator is adapted to respond to said received pad not being a next expected pad (page 18, 46, "A special re-synchronization procedure may be used to recover..").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Shefi as taught by Muller in order to provide integrity protection of signaling messages and on user traffic confidentiality over the wireless network.

9. As to claims 9 and 16, these are rejected using the same rationale as for the rejection of claim 2.

10. As to claim 3, Shefi discloses wherein said code exchanger comprises at least one communications network selected from the group of a telephone network, a

wireless data network, a Local Area Network, a Wide Area Network, and an Internet (column 19, lines 28-36).

11. As to claims 10 and 17, these are rejected using the same rationale as for the rejection of claim 3.

12. As to claim 4, Shefi doesn't explicitly disclose wherein client device reconfigurator is adapted to challenge said user with one or more methods selected from the group of requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

However, Muller discloses wherein client device reconfigurator is adapted to challenge said user with one or more methods selected from the group of requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response (page 26, which describes authentication result is computed by the MS from the serial number ESN of the handset and the first part of the mobile identification number).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Shefi as taught by Muller in order to provide integrity protection of signaling messages and on user traffic confidentiality over the wireless network.

13. As to claims 11 and 18, these are rejected using the same rationale as for the rejection of claim 4.

14. As to claim 5, Shefi discloses one-time pad cryptological table (column 4, lines 5-15). However Shefi doesn't explicitly disclose further comprise an expiration field for each entry; said code comparator is further configured to determine if said received pad is expired; said session grantor is configured to grant a session only if said received pad is unexpired; and said client device reconfigurator is adapted to respond to said received pad being expired.

However, Muller discloses further comprise an expiration field for each entry ("time variant parameter" –e.g. page 13); said code comparator is further configured to determine if said received pad is expired (Muller discloses this concept by teaching time variant parameter, -e.g. page 13); said session grantor is configured to grant a session only if said received pad is unexpired (Muller discloses this concept by teaching time variant parameter, -e.g. page 13, see also page 16); and said client device reconfigurator is adapted to respond to said received pad being expired (46, "A special re-synchronization procedure may be used..").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Shefi as taught by Muller in order to provide integrity protection of signaling messages and on user traffic confidentiality over the wireless network.

15. As to claims 12 and 19, these are rejected using the same rationale as for the rejection of claim 5.

16. As to claim 7, Shefi doesn't explicitly disclose wherein said service session grantor is further configured to require a second step of acknowledgment between said service security server and said client device before said entry is marked as "used". However, Muller discloses wherein said service session grantor is further configured to require a second step of acknowledgment between said service security server and said client device before said entry is marked as "used" ("authentication challenge" –e.g. page 16, page 46).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Shefi as taught by Muller in order to provide integrity protection of signaling messages and on user traffic confidentiality over the wireless network.

17. As to claims 14 and 21, these are rejected using the same rationale as for the rejection of claim 7.

18. Claims 6, 13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shefi in view of Muller and further in view of Douceur et al. (Patent Number: 6,021,203), hereinafter "Douceur".

19. As to claim 6, neither Shefi nor Muller explicitly discloses wherein said client device reconfigurator is adapted to replace said tables using a secure replacement method. However, Douceur discloses replacing tables using a secure replacement method (abstract, "secure channel").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Shefi and Muller as taught by Douceur in order to increase the confidentiality and integrity of the data. Furthermore, one would be motivated to do so to transmit data over the public netowork.

20. As to claims 13 and 20, these are rejected using the same rationale as for the rejection of claim 6.

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

- US 6891952 B1-Dynamic key generation and confidential synchronization of encryption component.
- US 594002 A – Security system with random number remote communication.
- US 5293576 A – Command authentication process.
- US 7009940 B2 – Integrity check in a communication system.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SP
SD

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100